
# PDSS™

# Personal Dynamic Security Shell ™

## Product Brief

# PDSS Description – Simply Dynamic Security and Ease of Use

PDSS™ provides a user-friendly dynamic authentication solution enhancing existing online, mobile, ATM , check transaction. It is perceived as the most effective tool against cyber weapons, be it hacking, key logging, spear phishing, malware, DdoS, phising, pharming. The cyber weapons have the silent power to destroy from power grids to military systems to our financial systems to our personal records to hacking our indispensable mobile devices. The dynamic authentication system is a "drop-in" solution which augments popular authentication systems, strengthening security while increasing usability. Studies show strong PDSS™ user adoption rates with a dramatic reduction in the possibility of unauthorized use and account takeover.

PDSS™ facilitates broad adoption by promoting trust and usability through greater user control and personalization over security questions, images, static identity and prompts. PDSS™ puts consumers in control so that dynamic identity is easy to setup, use and remember. Support for dynamically changing identity (images, phrases or characters) add to the security of PDSS™. Operational and fraud costs drop as users streamline their own added security.

The PDSS™ product Sherman™ can be completely customized per client needs. Applications are presented below for online scenarios, while mobile, ATM, and check printing and other applications are discussed in separate briefs. The technology can be applied across the board from from power grids to military systems to our financial systems to our personal records to hacking our indispensable mobile devices Contact **Protect Your Password** for a live demo.

## Sherman™ Authentication

In its simplest form in the demo on the site, users may chose a rule phrase that dynamically changes value of Day of the Week, month of the year, middle 2 digits of SSN, etc. The solution can be customized around many such combinations.

For example, during customer registration, a user may select "Day of the week" and list a challenge phrase "Every? I go to gym" and set **?** to "today+1". Using this rule, the correct password for log-in on Wednesdays will be "Every Thursday I go to Gym". In this example, the “+1” rule is the only thing a user will have to remember as her key for her password. Thus, every time the user logs in the system, she will have a dynamic password that is easy to remember, yet more secure than current best practices.

# Background

Mr. Obama has quoted a figure of $1 trillion lost last year to cybercrime--a bigger underworld than the drugs trade, though such figures are disputed. Banks and other companies do not like to admit how much data they lose. In 2008 alone Verizon, a telecoms company, recorded the loss of 285 million personal data records, including credit card and bank account details, in investigations conducted for clients. The cyber crime attacker might prefer to go to after unclassified military logistics supply systems or even the civilian infrastructure. A loss of confidence in financial data and electronic transfers could cause economic upheaval. These cyber weapons have the silent power to destroy from power grids to military systems to our financial systems to our personal records to hacking our indispensable mobile devices.

There are a several highly secure online authentications mechanisms commercially available, yet they have minimal consumer adoption and security for the following reasons:

- None of them are dynamic and can be penetrated too easily by hackers who are growing sophisticated day by day.
- Difficult to recall many unique passwords and challenge questions/responses and thus setting up the same one on all systems.
- Cumbersome to physically carry unique Secure ID cards for every account.
- Some solutions constrain consumers to using a specific computer.
- Hard to persuade consumers to change passwords on a regular basis.
- Social Networking makes it easier for static identities to be stolen

**The common attribute among all existing systems is that they are not dynamic and thus unreliable.** PDSS makes it dynamic and at the same time easy to use.

## Use Cases

***Online:*** The Wall Street Journal reported Sep 22, 2007 that US credit card institutions incurred a record **$1.24 billion** in fraud losses last year, up 9.3% from 2005. The primary cause of fraud is identified as customers' account information stored on the merchants' systems, falling into the wrong hands.

PDSS addresses this form of fraud. Even with stolen ID information, ID thieves would still be missing a vital piece of information (Sherman™ dynamic password) to successfully transact using the compromised customer accounts – thus these billion-plus dollar losses could have been prevented.

***Mobile:*** Selecting a favorite sentence or tune from a list increases security without undue usability issues for end consumers. See PDSS™ Mobile Security brief.

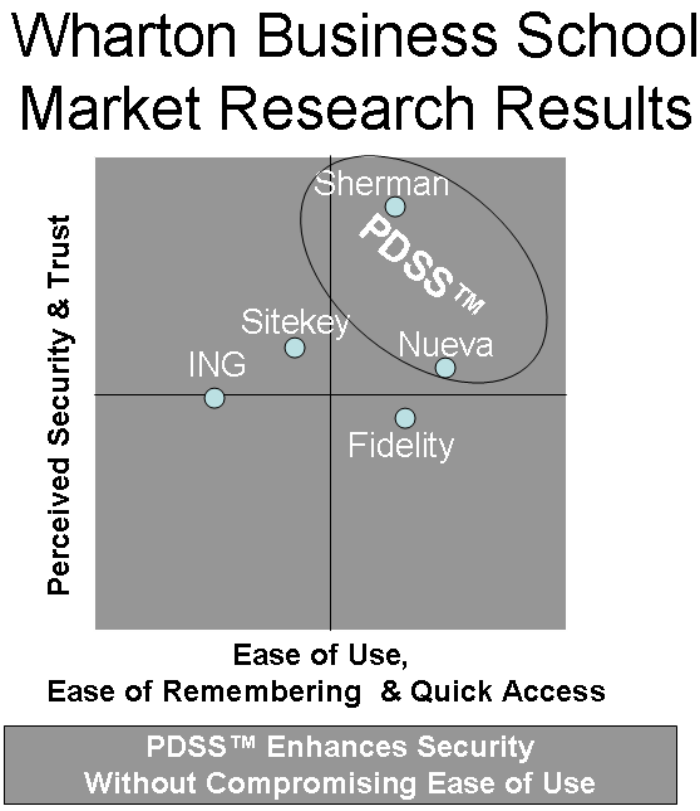
***ATM:*** Pins are often stolen, but dynamic answers to personalized questions cannot be. See PDSS™ Dynamic ATM brief.

***Checks:*** Dynamically changing watermarks reduce risk of illegitimate checks being cashed based on previously printed checks. See PDSS™ Check Printing brief.

***Cybercrime in general:*** Dynamically changing identity makes it hard to penetrate the systems.

## Market Research

The following market research study on Sherman™ was conducted at Wharton School of Business. In this study, five systems were selected for evaluation – Fidelity a traditional User Name and Password System, Bank of America's SiteKey, ING's Virtual pad system, and the Neuva™ and Sherman™ System. Neuva™ system is also part of PDSS portfolio but is picture based and dynamic as well. These were evaluated via survey following a series of focus group discussions, interviews with potential customers, and secondary research.




The study-validated consumers are looking for an easy to use system with the highest security possible. The Sherman™ system was perceived by the users to be at least as easy to use as traditional user name password systems used by Fidelity but Neuva™ was perceived to provide highest security.

PDSS™ provides the following competitive advantages:

- Enhanced level of security
- Ease of use not compromised
- Easy to personalize challenges and configure for dynamically changing passwords
- Higher consumer confidence due to users physically verifying each step vs. operators configuring algorithms which consumers have no say over.

For more information, please contact **Protect Your Password (USA)** by visiting the Contact Us Page.